

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title

ATTACHMENT A
Property to be Searched

The property to be searched N55W17943 High Bluff Dr, Unit C, Menomonee Falls, WI 53051, depicted below:



ATTACHMENT B
Items to be Seized

All records relating to violations of 21 U.S.C. §§ 841(a)(1), including but not limited to:

1. Marijuana, and any other controlled substance, packaging materials and materials used to prepare heroin and other controlled substances for distribution, controlled substances paraphernalia, and other contraband related to drug trafficking and distribution;
2. Firearms including pistols, handguns, shotguns, rifles, assault weapons, machine guns, magazines used to hold ammunition, silencers, components of firearms including laser sights and other components which can be used to modify firearms, ammunition and ammunition components, bulletproof vests, and any and all documentation related to the purchase of such items;
3. Proceeds of drug trafficking activities, including United States Currency, financial instruments, jewelry, documents and deeds reflecting the purchase or lease of real estate, vehicles, jewelry or other items obtained with the proceeds from organized criminal and drug trafficking activities;
4. Drug or money ledgers, drug distribution or customer lists, drug supplier lists, correspondence, notations, logs, receipts, journals, books, records and other documents noting the prices, quantity, and/or times when controlled substances were obtained transferred or sold distributed, and/or concealed;
5. Indicia of occupancy, residency or ownership of the premises and things described in the warrant, including but not limited to utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease or rental agreements, addressed envelopes, escrow documents and keys.
6. Cellular telephones and all electronic storage areas on the device including text messages, contact lists, digital video recordings or other areas that may contain evidence of drug trafficking or firearm possession or use.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user’s state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER’s Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Case No.24-923M(NJ)

N55W17943 High Bluff Dr, Unit C, Menomonee
Falls, WI 53051

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the _____ Eastern _____ District of _____ Wisconsin _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. 841(a)(1)	Distribution of controlled substances.

The application is based on these facts:

See attached affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



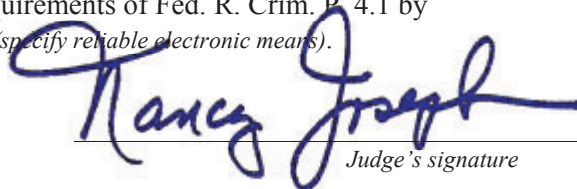
Applicant's signature

FBI SA Jacob A. Dettmering

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
_____ telephone _____ (specify reliable electronic means).

Date: 9/20/2024



Judge's signature

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Jacob A. Dettmering, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as N55W17943 High Bluff Dr, Unit C, Menomonee Falls, WI 53051, hereinafter “Subject Premises,” further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and have been since January 7, 2018. I was assigned to the FBI Capital Area Gang Task Force (CAGTF) in Baton Rouge, Louisiana from June 15, 2018, to April 1, 2020. Since April 1, 2020, I have been assigned as the Task Force Coordinator for the Milwaukee Area Safe Streets Task Force (MASSTF). Since 2018, I have investigated violations of federal law, directed drug and street gang investigations, obtained and executed search and arrest warrants related to the distribution of illegal narcotics, and debriefed confidential informants and cooperating defendants. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), in that I am empowered by law to conduct investigations of and to make arrests for federal offenses.

3. I have been trained in a variety of investigative and legal matters, including the topics of Fourth Amendment searches, the drafting of search warrant affidavits, and probable cause. I have participated in criminal investigations, surveillance, search warrants, interviews, and

debriefs of arrested subjects. As a result of this training and investigative experience, I have learned how and why violent actors typically conduct various aspects of their criminal activities.

4. The facts in this affidavit come from my training and experience, my review of documents and information obtained from other agents/law enforcement officers. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all my knowledge about this matter.

5. Since February 2021, the ATF, Milwaukee Police Department (MPD), Federal Bureau of Investigation (FBI), and Drug Enforcement Administration (DEA) have been investigating identified members of the “Wild 100’s”, a violent street gang in Milwaukee, also known as the “Shark Gang”, including Deautris MATTISON, (DOB 11/17/1996), among others, for distribution of controlled substances and federal program fraud. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that Deautris MATTISON has committed violations of 21 U.S.C. § 841(a) (Possession with Intent to Distribute and Distribution of Controlled Substances).

PROBABLE CAUSE

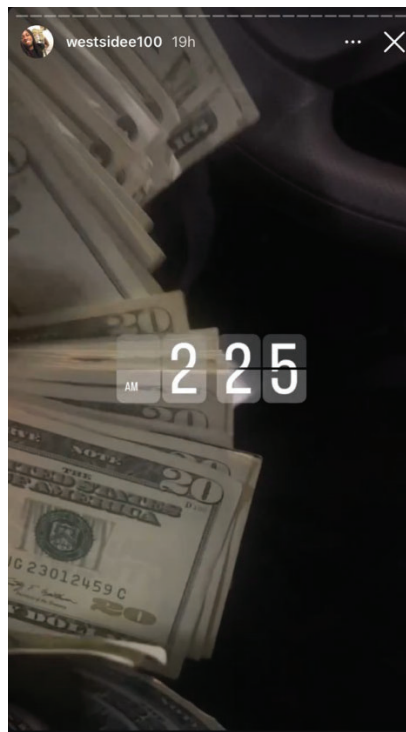
6. Deautris MATTISON, an identified member of the Wild 100s street gang, was arrested in connection with an arrest warrant based upon the sealed indictment returned in 23-CR-77, charging MATTISON along with 29 co-defendants, with violations of Title 18, United States Code, Sections 1341 (mail fraud) & 1349 (mail fraud conspiracy). On, July 2, 2024, MATTISON was released on conditions.

7. While MATTISON has been out of custody, case agents have monitored his social

media postings and have conducted physical surveillance.

8. Since the start of the investigation in 2020, case agents have been monitoring MATTISON's social media profile, which has now been changed to (Instagram: "Westsidee100"). Case agents have observed MATTISON posting numerous pictures of large amounts of cash, jewelry, and marijuana.

9. On July 7, 2024, MATTISON posted an Instagram story, which was a picture taken inside a vehicle based upon the steering wheel in the background of the picture. The picture itself depicts several hundred dollars, all in \$20 denominations fanned out, with the time stamp, "2:25am". A screenshot is set forth below.



10. Also on July 7, 2024, MATTISON posted several photos to his account, which show him standing in the middle of the street at 104th Court and Kiehnau Avenue, Milwaukee,

WI. It should be noted that the Wild 100's criminal street gang consider this area to be their territory. The photos showed MATTISON with designer clothing, a custom chain and pendant and displaying a stack of US currency in \$20 denominations. The caption on the post writes, "SAY LESS DO MORE!! IM BACK FOR A LIL MIN". Below the caption, he wrote the hashtag, "#FOREVERBOSS FREE DA GUYS", which Investigators know to mean, free the incarcerated members of the Wild 100's criminal street gang who were also indicted in May 2023. Screenshots are set forth below.





11. On July 9, 2024, MATTISON posted a story which showed him sitting inside a vehicle wearing a white t-shirt, and black hat. MATTISON was wearing his custom chain and pendant which read, “SNG RIP POPS”. Additionally, MATTISON was wearing a pair of custom Cartier glasses which have custom inscription of the photo of a Shark and reads “Westside”. Investigators know that the Wild 100 criminal street gang also went by “Shark Gang” and would often use the shark logo as branding. Westside refers to the West side of the city, which is often referred to as the “Hundreds”, which the gang would claim as their territory. A screenshot is set

forth below.

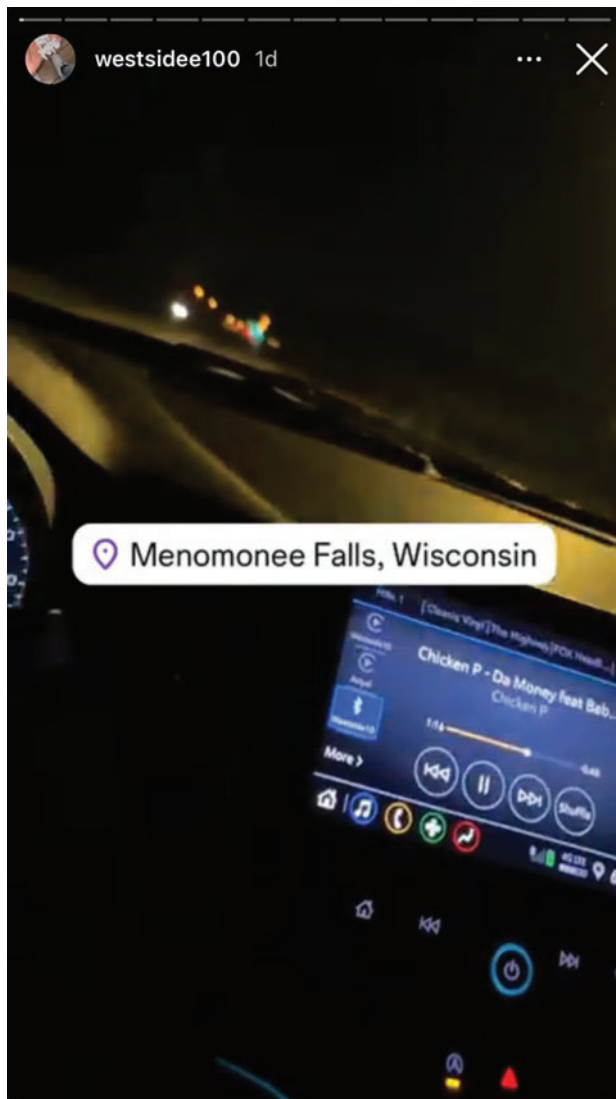


12. On July 10, 2024, at approximately 10:00pm, MATTSION posted a picture to his story which showed over 42 shoe boxes in a closet. The boxes ranged from Nike to Yeezy by Adidas, to Lanvin of Paris. The caption on the photograph stated, “We don’t move like street N*****, We been movin’ like a mob”. Investigators know that Yeezy’s on average cost

between \$100 and \$500 per pair. Additionally, Lanvin of Paris typically retail for around \$1,000 per pair. A screen shot of the post is set forth below.

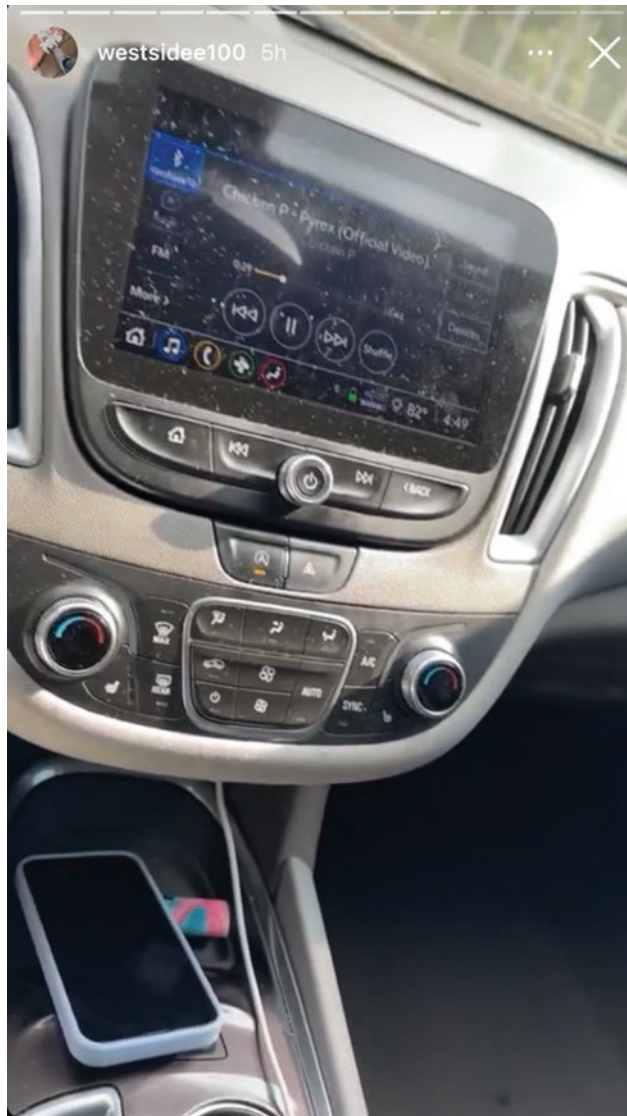


13. On August 11, 2024, MATTSION posted a picture of the inside of a vehicle showing the road in front from the vantage point of the driver's seat. The location tag on the photo read, "Menomonee Falls, Wisconsin". Immediately following that photo, he posted another photo, also from the driver's seat of a car. The picture showed the vehicle was backed into a garage and you could see three other garages across from his with two doors, depicting a condo/apartment complex. The following photo posted was a ceiling showing a ceiling fan. In the photo, it could be seen that there was a smoke detector on the ceiling but also a sidewall mounted fire protection sprinkler head. Your affiant knows that fire protection systems are required by the Uniformed Fire Code for multifamily condos and apartments. It is rare to see a residential fire protection sprinkler system in single family houses. Screenshots are set forth below.





14. On the same day, MATTSION also posted pictures to his story from inside his vehicle. One of which just showed the dash of the vehicle and the area below the dash. Located in the area below the dash was an Apple iPhone with a light blue colored case. It appeared as MATTSION was alone as there were no feet shown on the floorboard on the passenger side of the vehicle. Investigators believe that the phone would be a second phone for MATTISON, since the picture was likely taken from his other phone. A screenshot is set forth below.



15. Later, MATTISON posted a picture of himself in the car. MATTISON appeared to have one hand on the steering wheel and was shirtless. He was wearing a light-colored hat and still had his custom chain and pendant around his neck which read, “SNG RIP POPS”, and was wearing his Cartier glasses on his face.



16. The next photo posted to his story was a picture of the cupholder area of his vehicle which showed the Apple iPhone with light blue case and had the caption, “Good smoke hit me!!”. Investigators know that mobile drug dealers very commonly have numerous phones. They typically have one which is used primarily for personal use and the others are typically used for drug sales and communication with their drug customers and/or supplier(s). Investigators also know that “good smoke” is commonly used to refer to good Marijuana. Investigators further believe that the entire caption is telling customers that he has good Marijuana and to call him on

the pictured telephone to buy some from him. A screen shot is set forth below.



17. On August 17, 2024, at approximately 6:45pm, MATTISON posted a picture to his Instagram story which showed the middle console of a vehicle, and it was taken from the vantage point of the driver's seat. The picture showed a light blue colored Apple iPhone, a dark colored iPhone, and two "flip phones". It should be noted that the picture was taken from an additional phone not pictured. The photograph also had a location tag which showed "Mill Road".

Investigators know this to be the territory claimed by the Wild 100's criminal street gang. A screenshot is set forth below.



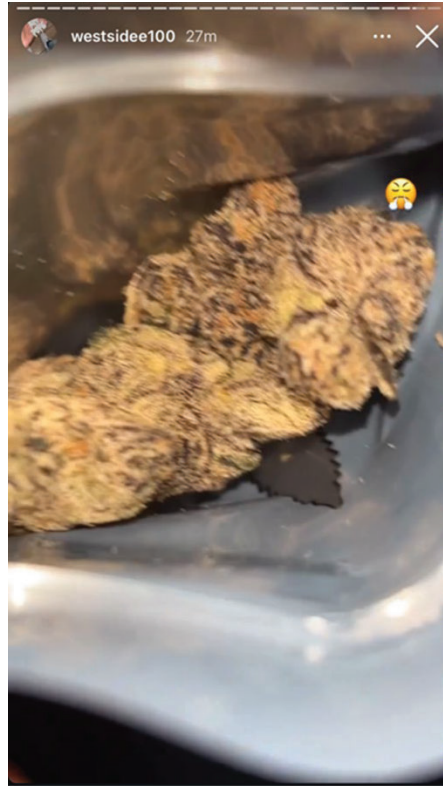
18. Additionally, license plate readers were searched for the white Chevy Malibu bearing Wisconsin license plate AWL6526, believed to be driven by MATTISON. The vehicle was located by one at 6:26pm, travelling westbound on North Avenue at 61st street, Milwaukee, WI. At 7:01pm, it was seen travelling westbound on Silver Spring Drive at Campbell Drive, Menomonee Falls, WI. At the time of the Instagram photo, the Malibu could have been in the area of Mill Road, based upon the license plate readers.

19. On August 18, 2024, at approximately 9:20pm, MATTISON posted a video of him driving down the road. The video showed a vehicle passing houses and streetlights. The video had emojis of 5 people, of all different ages, sex, and races. Investigators believe that post indicated that MATTISON was out selling drugs to different people of all walks of life. A screenshot is set forth below.

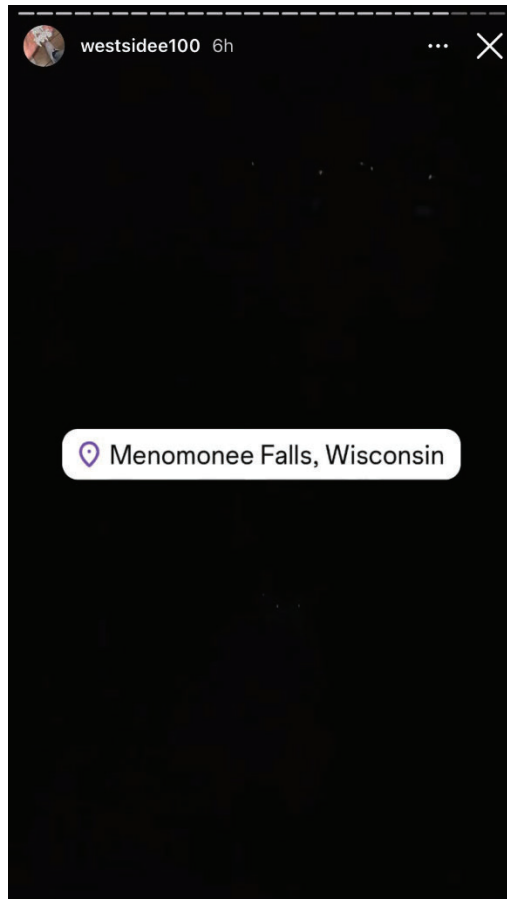


20. On August 19, 2024, at approximately 8:00pm, MATTISON posted a photograph to his Instagram story which showed what appeared to be Marijuana inside a commercially packaged 3.5-gram Marijuana container. Investigators believe that this is in reference to MATTISON's August 12, 2024, post which referenced having "good smoke". Investigators know that it is common for drug traffickers to post to social media looking for potential customers, and

part of that involves posting pictures of the product, in this case, Marijuana. A screenshot is set forth below.



21. On August 20, 2024, at approximately 2:00am, MATTISON posted a video to his Instagram story which was very dark but is believed to be a video taken from inside a vehicle, looking out a window as the vehicle is travelling. The video had a geolocation tag which read, “Menomonee Falls, Wisconsin”. Investigators believe that MATTISON was heading home to the Subject Premises for the night. Investigators know that the last license plate reader hit was at 1:44am, westbound on Mill Road from Parkway Drive, which would indicate driving towards Menomonee Falls, WI. A screenshot is set forth below.



22. On August 25, 2024, at approximately 2:30pm, MATTISON posted a picture to his Instagram story which showed what appeared to be Marijuana inside a commercially packaged 3.5-gram Marijuana container. Immediately following, MATTISON posted a selfie of himself to his Instagram where MATTISON could be seen wearing the “SNG RIP POPS” chain and pendant.



23. On August 26, 2024, MATTISON posted three pictures to his story, the first was the interior of a closet which appeared to have lots of designer clothing and shoes. The estimated value of all of it is more than \$10,000. The second was of his Nike shoes with the captions, “GM” and “Get Money!!!!” The third was a selfie with MATTISON wearing a white tank top, wearing his chain and pendant and Cartier sunglasses. Screenshots are set forth below.





24. On August 29, 2024, MATTISON posted a picture of the middle console of his vehicle which showed an ash tray in the front cup holder and two flip phones in the rear cup holder. The picture had the caption, “TOP OF THE MORNING!!!!”. A screenshot is set forth below.



25. On August 30, 2024, MATTISON posted a video to his Instagram story which depicted him driving in a vehicle down the road. The video had an emoji which depicted a stack of money with wings. Investigators believe this is in reference to making money while mobile dealing drugs. A screenshot is set forth below.



26. On August 30, 2024, at approximately 2am, MATTSION posted a video to his Instagram story, which was taken from the interior of a vehicle, shot from the driver's seat. The video showed the vehicle parked in a garage with the garage door closing. The video had the text, "Love" with a peace sign emoji. Investigators believe this was referencing being in for the night

after being out in the streets mobile dealing. It should be noted that Investigators know the video taken was from the garage for N55W17943 High Bluff Dr, Unit C, Menomonee Falls, WI. A screenshot is set forth below.



IDENTIFICATION OF RESIDENCE

27. Investigators obtained a Pen Register/Trap and Trace order (App No. 16301) from the Honorable Magistrate Judge, William Duffin, on July 10, 2024, for MATTISON's account, "westsidee100".

28. Investigators reviewed the logins for the account and were able to identify IP address logins for the account with the specific dates and times of the logins. Specifically, Investigators sent a Subpoena to AT&T U-Verse for seven (7) IP address logins for MATTISON's account.

29. On August 11, 2024, AT&T returned results for the Subpoena. All seven (7) of the IP address logins were made from the address, N55W17943 High Bluff Dr, Unit C, Menomonee Falls, WI. The subscriber for that account was Audrey BUCKNER. Investigators are not aware of the connection between BUCKNER and MATTISON currently. However, Investigators know based upon training and experience that many gang members and drug dealers utilize females as subscribers for internet, utilities and many times, rental vehicles to conceal their involvement in illicit activities.

30. On August 12, 2024, Investigators conducted physical surveillance at the residence and found that it was a large, new construction, multi-family townhome, called High Bluff at Creekwood Crossing. Investigators identified the location for the garage to "Unit C" and saw that the vantage point from that garage would see across to three other garages and two doors as depicted in the screenshot in paragraph 26. Below is a picture of one of the buildings which you can see the two doors in the middle and three garages to each side.



31. Additionally, Investigators were able to access the website for the town homes and take a virtual 3D tour of a unit which would be a mirrored image to Unit C.

32. On August 14, 2024, at approximately 6:22pm, physical surveillance being done on the residence witnessed a white Chevy Malibu bearing Wisconsin license plate AWL6526, exit the garage for N55W17943 High Bluff Dr, Unit C, Menomonee Falls, WI. Surveillance followed the vehicle, which was heavily tinted and saw a black male subject matching the physical descriptors of MATTISON, driving the vehicle. It should be noted that the vehicle was backed into the garage and as it exited, it appeared to use a garage door opener within the vehicle to close the garage door. It should be noted that the Chevy Malibu bearing Wisconsin license plate AWL6526 is registered to Audrey Marie BUCKNER, same at the internet subscriber for N55W17943 High Bluff Dr, Unit C, Menomonee Falls, WI.

33. On August 16, 2024, at approximately 7:42pm, physical surveillance was being conducted on N55W17943 High Bluff Dr, Unit C, Menomonee Falls, WI. A white Chevy Malibu,

bearing Wisconsin license plates AWL6526, arrived at the residence, opened the garage door remotely and backed into the garage. The tint on the vehicle was very dark, but a black male subject matching the physical descriptors of MATTISON could be seen through the windshield, operating the vehicle.

34. On August 18, 2024, MATTISON posted a video to his Instagram page which was from the view of the driver's seat of what appears to be a Chevy Sedan. The video showed the garage door closing with a "Peace sign" emoji in the corner. The background of the video showed the garage across from MATTISON, which all had cars parked in front of them. Investigators conducted surveillance on N55W17943 High Bluff Dr, Unit C, Menomonee Falls, WI, and could confirm that the vehicles parked there matched the appearance of those depicted from the video. Based on that video and the direction in which it was taken, Investigators could determine it was the Garage for unit C. The screenshot is set forth below.



35. On August 26, 2024, MATTISON was seen via physical surveillance, leaving N55W17943 High Bluff Dr, Unit C, Menomonee Falls, WI, driving the white Chevy Malibu, bearing Wisconsin license plate AWL6526.

36. On September 6, 2024, MATTISON posted two pictures to his Instagram story. The first was a picture of the business counter of an Enterprise rental car. The second was the interior of a newer vehicle. Clorox disinfecting wipes and a pamphlet could be seen in the cup holders which is consistent with a rental car. Case agents called the Enterprise Law Enforcement

contact and confirmed that MATTISON rented a White 2024 Volks Wagon ACSP, bearing Wisconsin fleet plate 23971AFT. The rental was picked up on September 6, 2024, and due back on September 9, 2024.

37. On September 6, 2024, MATTISON was seen via electronic surveillance, arriving at N55W17943 High Bluff Dr, Unit C, Menomonee Falls, WI, driving a white Volks Wagon SUV. MATTISON opened the garage door via a garage door opener which was located within the vehicle. MATTISON could be seen exiting the driver's seat of the vehicle and entering the garage while wearing a bright orange sweatshirt and black pants with an orange stripe. After a short while, MATTISON came back outside, entered the vehicle, closed the garage door remotely, and left the area.

38. On Thursday, September 19, 2024, at approximately 1:43 am, MATTISON posted a video to his Instagram account which showed him inside the driver's seat of a vehicle. The vehicle was inside a garage and the garage door was closing. Based upon my experience and knowledge of the investigation, I know that garage to be associated with N55W17943 High Bluff Dr, Unit C, Menomonee Falls, WI, based upon the apartment across from the garage, which can be seen in the post. Additionally, Investigators have electronic surveillance on the address, and you could see a vehicle arrive at approximately 1:42 am and back into the garage at 1:43 am. A screenshot of the post is set forth below:



39. Case agents are aware based upon their training and experience and the investigation to date, that drug traffickers commonly maintain evidence of their drug trafficking, including drug ledgers, financial documents, U.S. currency, cellular telephones, customer contact information, jewelry or other items purchased with drug proceeds, in their homes or “stash” houses. Case agents are also aware it is common practice for individuals who are involved in business activities of any nature to maintain books and records of such business activities for lengthy periods of time. Because narcotics trafficking generates large sums of cash, it requires the

keeping of detailed records as to the distribution of narcotics as well as the laundering of the proceeds. Such records also typically provide evidence as to the identity of additional criminal associates who are facilitating the laundering of the narcotics proceeds on behalf of the organization. These records, unlike controlled substances, are often maintained for long periods of time, even several years, based on case agents' training and experience. It is also common practice for individuals who maintain these records to keep them in places that are secure but easily accessible such as in their businesses or personal residences.

- a. I have learned about the manner in which individuals and organizations distribute controlled substances in Wisconsin as well as in other areas of the United States;
- b. I am familiar with the coded language utilized over the telephone to discuss drug trafficking and know that the language is often limited, guarded and coded. I also know the various code names used to describe controlled substances;
- c. I know drug traffickers often purchase and/or title their assets in fictitious names, aliases or the names of relatives, associates or business entities to avoid detection of these assets by government agencies. I know that even though these assets are in the names other than the drug traffickers, the drug traffickers actually own and continue to use these assets and exercise dominion and control over them;
- d. I know drug traffickers must maintain on-hand, large amounts of U.S. currency in order to maintain and finance their ongoing drug business;
- e. I know it is common for persons involved in drug trafficking to maintain evidence pertaining to their obtaining, secreting, transfer, concealment and/or expenditure of drug proceeds, such as currency, financial instruments, precious metals and gemstones, jewelry, books, records of real estate transactions, bank statements and records, passbooks, money drafts, letters of credit, money orders, passbooks, letters of credit, bank drafts, cashier's checks, bank checks, safe deposit box keys and money wrappers. These items are maintained by the traffickers within residences, businesses or other locations over which they maintain dominion and control;
- f. I know it is common for drug traffickers to maintain books, records, receipts, notes ledgers, airline tickets, receipts relating to the purchase of financial instruments and/or the transfer of funds and other papers relating to the transportation, ordering, sale and distribution of controlled substances;

- g. It is common practice for individuals who are involved in business activities of any nature to maintain books and records of such business activities for lengthy periods of time. It is also common practice for individuals who maintain these records to keep them in places that are secure but easily accessible such as in their businesses, offices, or personal residence;
- h. It is also common that individuals who are attempting to conceal their true income from the IRS will maintain records that will establish their true ownership of assets or other expenditures in a secret manner. These records have included bank records, automobile titles, property deeds, cashier's check receipts, money order receipts, wire transfer receipts, documents pertaining to storage facilities or safe deposit boxes, documents or agreements detailing the true ownership of assets, photographs of the true owners with the concealed assets, or other items such as sales receipts, purchase orders, or shipping invoices;
- i. I know drug traffickers often use electronic equipment such as telephones, pagers, computers, telex machines, facsimile machines, currency counting machines and telephone answering machines to generate, transfer, count, record and/or store the information described in the items above, as well as conduct drug trafficking activities;
- j. I know when drug traffickers amass large proceeds from the sale of drugs, the drug traffickers attempt to legitimize these profits through money laundering activities. To accomplish these goals, drug traffickers utilize the following methods, including, but not limited to: domestic and international banks and their attendant services, securities brokers, professionals such as attorneys and accountants, casinos, real estate, shell corporations and business fronts and otherwise legitimate businesses which generate large quantities of currency;
- k. I know drug traffickers commonly maintain addresses or telephones numbers in books or papers which reflect names, addresses and/or telephone numbers of their associates in the trafficking organization;
- l. I am familiar with computers, cellular telephones, pagers and their uses by drug traffickers to communicate with suppliers, customers, and fellow traffickers and by those engaged in money laundering activities to communicate with their associates and financial institutions; That drug traffickers use these devices to record their transactions and aspects of their lifestyle related to drug dealing, whether in the form of voicemail, email, text messages, video and audio clips, floppy disks, hard disk drives, flash drives, CD's, DVD's, optical disks, Zip disks, flash memory cards, Smart media and any data contained within such computers or cellular telephones, electronic storage media and other settings particular to such devices; I know that such devices automatically record aspects of such communications, such

as lists of calls and communications, and any particularized identification assigned to those source numbers or email addresses by the owner of the devices; and

- m. Specifically, I know the following information can be retrieved to show evidence of use of the computer to further the drug trade and/or money laundering activities; Computer systems and cellular telephones, including but not limited to system components, input devices, output devices, data storage devices, data transmission devices, and network devices and any data contained within such systems; and computer media and any data contained within such media and other material relating to computer systems and the internet including but not limited to, documentation, operating system software, application or access program disks, manuals, books, brochures, or notes; and computer access codes, user names, log files, configuration files, and passwords, screen names, email addresses, IP addresses and cellular / wireless telephones, SIM cards, any removable storage devices for telephones, and any data contained therein, including but not limited to stored telephone numbers, recently called numbers list, text messages, digital audio and/or video recordings, pictures, settings, and any other user defined settings and/or data.

The Premises to be Searched

40. According to records from AT&T, Audrey BUCKNER is the account holder for internet supplied to the Subject Premises. MATTISON has been seen on numerous occasions driving the white Chevy Malibu, which is registered to BUCKNER. Additionally, Surveillance conducted from August through September 2024 showed MATTISON leaving the Subject Premises on several occasions.

41. There is probable cause to believe that evidence 21 U.S.C. § 841 (Distribution of Controlled Substances), will be located at the Subject Premises occupied by BUCKNER and MATTISON.

TECHNICAL TERMS

42. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

43. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Subject Premises, in whatever form they are found. One form in which the records might be found is data stored on a computer’s hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

44. I submit that if a computer or storage medium is found on the Subject Premises, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later

using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

45. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the Subject Premises because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record

information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating, or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user’s state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner’s motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a “wiping” program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

46. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of

information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

47. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

48. I submit that this affidavit supports probable cause for a warrant to search the Subject Premises described in Attachment A and seize the items described in Attachment B.

ATTACHMENT A
Property to be Searched

The property to be searched N55W17943 High Bluff Dr, Unit C, Menomonee Falls, WI 53051, depicted below:



ATTACHMENT B
Items to be Seized

All records relating to violations of 21 U.S.C. §§ 841(a)(1), including but not limited to:

1. Marijuana, and any other controlled substance, packaging materials and materials used to prepare heroin and other controlled substances for distribution, controlled substances paraphernalia, and other contraband related to drug trafficking and distribution;
2. Firearms including pistols, handguns, shotguns, rifles, assault weapons, machine guns, magazines used to hold ammunition, silencers, components of firearms including laser sights and other components which can be used to modify firearms, ammunition and ammunition components, bulletproof vests, and any and all documentation related to the purchase of such items;
3. Proceeds of drug trafficking activities, including United States Currency, financial instruments, jewelry, documents and deeds reflecting the purchase or lease of real estate, vehicles, jewelry or other items obtained with the proceeds from organized criminal and drug trafficking activities;
4. Drug or money ledgers, drug distribution or customer lists, drug supplier lists, correspondence, notations, logs, receipts, journals, books, records and other documents noting the prices, quantity, and/or times when controlled substances were obtained transferred or sold distributed, and/or concealed;
5. Indicia of occupancy, residency or ownership of the premises and things described in the warrant, including but not limited to utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease or rental agreements, addressed envelopes, escrow documents and keys.
6. Cellular telephones and all electronic storage areas on the device including text messages, contact lists, digital video recordings or other areas that may contain evidence of drug trafficking or firearm possession or use.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user’s state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER’s Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.